

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

REMARKS

The Office Action dated April 30, 2004 has been received and carefully reviewed. Claims 16 and 21 were amended to correct matters of form only. No new matter has been added. Accordingly, claims 1-23 are pending in this application and submitted for reconsideration.

Objections to the Claims:

Claims 16 and 21 were objected to because they contain the term "capable of." Each of claims 16 and 21 were amended to remove the term "capable of." Accordingly, the Applicant requests that the objection be withdrawn. This change is just cosmetic and, thus, will not change the scope of the claims nor limit the broadest reach of the claims under the doctrine of equivalents.

Rejection of the Claims:

Claims 9 and 11-12 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication No. 2004/0073612, Maria et al. ("Maria"). Applicant traverses the rejection and submits that claims 9 and 11-12 recite subject matter not shown or described by Maria.

At the outset, Applicant submits that Maria is not prior art to the present application. The present application was filed on October 18, 2000, and therefore Maria is only available as prior art as a publication having a prior art publication date of April 15, 2004. Nonetheless, Applicant addresses this rejection on the merits without prejudice since Maria claims priority to a number of prior granted patents.

Nevertheless, if the Patent Office seeks to change the rejection based on such prior granted patents, the Office is requested to issue a new rejection and Office Action.

Claim 9, upon which claims 11 and 12 depend, recites a method for preventing an unauthorized access to a network via a user computer which is connected to the network and to an access control system, the method comprising: storing an **IP address** of the user computer in a memory of the access control system; receiving a data packet from the user computer; comparing an originating **IP address** of the data packet with the **IP address** of the user computer stored in the memory of the access control system; and denying the user computer an access to the network if the originating **IP address** of the data packet is different from the **IP address** of the user computer stored in the memory of the access control system.

As a result, in some examples, untraceable malicious acts can be prevented and those responsible for such acts can be caught. The present invention can, *inter alia*, prevent individuals from accessing a network when they alter transmission logs or IP addresses of data packets. For example, such acts as "IP-spoofing" attacks, smurf attacks, teardrop attacks, etc. can be prevented.

In contrast, Maria is directed towards a method for filtering data packets. More particularly, Maria is directed to a high-performance data packet filter which can work with a large number of source IP addresses. Therefore, Maria includes a packet filter processor 14 which combines the elements of a high-speed microprocessor, a source IP address list stored in high-speed memory, and a dedicated proprietary operating system to ensure that data packets can be filtered at a high rate of speed. See Maria at paragraph 0025. Accordingly, Maria maintains these massive lists of IP addresses for the purpose of routing or dropping packets. Depending on the node, when a packet is received, it is dropped or passed if there is a match with the source IP list.

Thus, Maria functions different from, e.g., embodiments herein where, e.g., the source IP address of a packet coming from the user computer matches the stored IP address for that same user computer. By the method of such preferred embodiments, it can potentially be determined when a particular computer has changed its source IP

address. As a result, malicious acts can be prevented from the user computer. The filter described in Maria is incapable of determining when the source IP address of a data packet has been changed from the source IP address assigned to a particular computer. Thus, Maria fails to show or describe the combination of features recited in claim 9, upon which claims 11-12 depend. Accordingly, Applicant requests that the rejection be withdrawn and claims 9 and 11-12 be allowed.

Claims 1-8, 10, 13-15 and 16-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Maria. Applicant respectfully traverses the rejection and submits that Maria fails to show or suggest each and every element of claims 1-8, 10, 13-15 and 16-23.

Claim 1, upon which claims 2-4 depend, recites an access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising: a memory containing an **IP address** assigned to the user computer; and a microprocessor programmed to terminate a connection between the user computer and the network when an originating **IP address** of a data packet received from the user computer does not match the **IP address** assigned to the user computer that is contained in the memory.

Claim 5, upon which claims 6-8 depend, defines an access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system, the system comprising: a memory containing an **IP address** assigned to the user computer; and a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating **IP address** of a data packet received from the user computer does not match the **IP address** assigned to the user computer that is contained in the memory, wherein the access control system is located between the user computer and the host computer system.

Claim 13 defines a method of preventing an unauthorized access to a network via a user computer connected to the network through a host computer system which is connected to an access control system, the method comprising: storing an **IP address** of the user computer in a memory of the access control system; receiving a data packet from the user computer; comparing an originating **IP address** of the data packet with the **IP address** of the user computer stored in the memory of the access control system; and terminating a connection between the user computer and the host computer system if the originating **IP address** of the data packet is different from the **IP address** of the user computer stored in the memory of the access control system.

Claim 16, upon which claims 17 and 19 depend, defines a secure network comprising: a host computer system connected to the secure network; an access control system connected to the host computer system and having a memory; and a user computer connected to the host computer system and configured to access the secure network through the host computer system, wherein the memory of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating **IP address** of a data packet sent from the user computer for transmission to a node in the secure network does not match the **IP address** of the user computer contained in the memory of the access control system.

Claim 20 defines a secure network comprising: a user computer connected to the secure network; and an access control system connected to the user computer and having a memory, wherein the memory of the access control system contains an **IP address** assigned to the user computer, and wherein the access control system is programmed to deny the user computer an access to the secure network when an originating **IP address** of a data packet sent from the user computer for transmission to a node in the secure network does not match the **IP address** of the user computer contained in the memory of the access control system.

Claim 21, upon which claims 22 and 23 depend, defines an access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising: a memory containing an **IP address** assigned to the user computer; and a comparator structure configured to terminate a connection between the user computer and the network when an originating **IP address** of a data packet received from the user computer does not match the **IP address** assigned to the user computer that is contained in the memory.

As described above, with respect to claim 9, Maria fails to disclose storing an IP address assigned to a user computer and comparing the originating IP address of a data packet received from that user computer with the stored IP address assigned to the user computer, and then denying the user computer an access to the network.

The Maria reference very clearly does **not** teach or suggest a number of recitations recited in the claims. The preferred embodiments of the present invention enable, e.g., determination of when the user computer has altered its IP address from the IP address assigned. Maria fails to disclose or suggest such capabilities. On the other hand: **claim 1** recites the feature of a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address

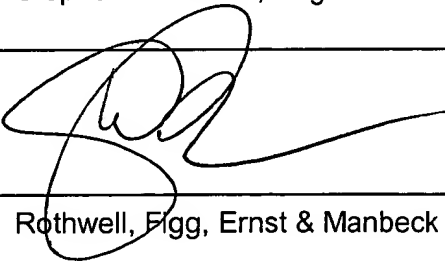
assigned to the user computer that is contained in the memory; **claim 5** includes a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory, wherein the access control system is located between the user computer and the host computer system; **claim 16** recites that the memory of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system; **claim 20** recites that the access control system is programmed to deny the user computer an access to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system; **claim 21** includes a comparator structure configured to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

Further, it was suggested in the Office Action that it would have been obvious to one of ordinary skill in the art to modify Maria to terminate a connection between the user computer and a host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer. In the Office Action, it is asserted that Maria discloses terminating a connection. However, the packet filter processor 14 of Maria is implemented between the physical layer and the data link layer. See paragraph 0037 of Maria. The network layer is the layer concerned with routing data from one network node to another and is responsible for establishing, maintaining, and terminating the network connection between two users and for transferring data along that connection. Nowhere does Maria suggest communicating with the network layer of the network device, and, therefore, Maria actually teaches away from terminating a connection between computers and the network. "Therefore, by implementing packet filter processor 14 between the physical layer and the data link layer, processor 14 can maximize the speed at which it filters each packet." See paragraph 37 of Maria. Because Maria is concerned with the speed of filtering packets within the network, one having ordinary skill in the art would not be motivated to modify the invention to perform the extra steps necessary to derive the present invention.

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

Accordingly, in view of the above, applicant submits that Maria fails to show or suggest the combinations of features recited, respectively, in claims 1-8, 10, 13-15 and 16-23 and that one having ordinary skill in the art would not have been motivated to modify Maria in order to cure the deficiencies described above. Thus, the Applicant submits that claims 1-8, 10, 13-15 and 16-23 are in condition for allowance and requests that the rejection be withdrawn and that claims 1-4, 5-8, 10, 13-15 and 16-23 be allowed.

In the event that this paper is not timely filed, the Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account No. 02-2135.

RESPECTFULLY SUBMITTED,					
NAME AND REG. NUMBER	Stephen B. Parker, Registration No.: 36,631				
SIGNATURE				DATE	8/19/04
ADDRESS	Rothwell, Figg, Ernst & Manbeck Suite 800, 1425 K Street, N.W.				
CITY	Washington	STATE	D.C.	ZIP CODE	20005
COUNTRY	U.S.A.	TEL.:	(202) 783-6040	FAX	(202) 783-6031